Case Study : Phishing Attack

CYBERSECURITY
IBM
Network Security & Database Vulnerabilities
Powered By
coursera
IBM Digital Credential

Adobe

Data Breach

Company Description

Company Information:

Industry: Software
Valuation: $27.24 billion (2021)
Employee: 25,988 (2021)
Location: United States

- Adobe Inc. originally called **Adobe Systems Incorporated**, is an American multinational computer software company incorporated in Delaware and headquartered in San Jose, California. It has historically specialized in software for the creation and publication of a wide range of content, including graphics, photography, illustration, animation, multimedia/video, motion pictures, and print. Its flagship products include Adobe Photoshop image editing software; Adobe Illustrator vector-based illustration software; Adobe Acrobat Reader and the Portable Document Format (PDF)
- Adobe was founded in December 1982 by John Warnock and Charles Geschke, who established the company after leaving Xerox PARC to develop and sell the PostScript page description language. In 1985, Apple Computer licensed PostScript for use in its LaserWriter printers, which helped spark the desktop publishing revolution. Adobe later developed animation and multimedia through its acquisition of Macromedia, from which it acquired Adobe Flash; video editing and compositing software with Adobe Premiere, later known as Adobe Premiere Pro; low-code web development with Adobe Muse; and a suite of software for digital marketing management.
- Source: Wikipedia Adobe Inc. – Wikipedia In *Wikipedia*

Attack Category

A data exposure of 7 million Adobe Creative Cloud account records could put users at risk of targeted phishing.

Description of the Attack :

Nearly 7.5 million Adobe Creative Cloud user records were left exposed to anyone with a web browser, including email addresses, account information, and which Adobe products they use.

October 19, 2019 – Security researcher Diachenko discovered the exposed data and immediately notified Adobe.

Comparitech partnered with security researcher Bob Diachenko to uncover the exposed database. The **Elasticsearch database** could be accessed without a password or any other authentication.

Spear-phishing warning

However, it is unclear if someone else also accessed this database and downloaded its content. The data inside could be used to send spam to users who had their email addresses exposed. Specifically, hackers could target owners of active Adobe premium accounts with **phishing emails** to hijack high-value Creative Cloud accounts from owners, which they can later re-sell online.

Risk Assessment Report

Learning Outcome:

Develop a cyber security risk mitigation strategy specific to the organization

1.0 Introduction

1.1 Purpose

- A Risk assessment should be done to determine vulnerabilities within the organization

1.2 Scope of the security risk assessment

- Specify what systems , networks and applications were reviewed as part of the security assessments.
- Determine the role and responsibilities of the team leaders.
- The cost of the security breach and the prevention of further breaches

1.3 Vulnerability sources

- The assessment team will use vulnerabilities sources to help identify potential vulnerabilities

Roles and Responsibilities

NIST Guidelines

Learning outcomes:

Project team should follow the guidelines outlined in the NIST Cybersecurity Framework

www.nist.gov/cyberframework

- Identify- Protect- Detect

- Respond- Recover

Role	Responsibilities
Risk or Project Manager	The Risk Manager identifies risks, verifies if the risk is internal or an external threat.
Integrated Project .Team	This team is responsible for identifying the risks, determining the impact, timing, and priority of the risks.
Risk Owner(s)	The risk owner determines which risks require mitigation and contingency plans. They perform a cost benefit analysis of the proposed strategies. They are also monitoring, controlling and updating the status of the risk.
Other Key Stakeholders	They assist in identifying and determining the context, consequence, impact, timing and priority of the risk.

Vulnerabilities

Vulnerability #1

AEM's Cloud Service offering, as well as version 6.5.10.0 (and below) are affected by a reflected Cross-Site Scripting (XSS) vulnerability via the item ResourceType parameter.

Summary

If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.

Vulnerability #2

Adobe Commerce versions 2.4.3-p2 (and earlier), 2.3.7-p3 (and earlier) and 2.4.4 (and earlier) are affected by an Improper Access Control vulnerability that could result in a Security feature bypass

Summary

An attacker could leverage this vulnerability to leak minor information of another user's account details. Exploitation of this issue does not require user interaction.

Costs & Prevention

Cost

- An agreement in August 2015 called for Adobe to pay $1.1 million in legal fees and an undisclosed amount to users to settle claims of violating the Customer Records Act and unfair business practices.
- In November 2016, the amount paid to customers was reported to be $1 million.

Prevention

- Comparitech conducts security research that entails scanning the web for exposed databases. When we uncover a database that hasn't been properly secured and allows unauthorized access, we immediately notify the owner.
- Our aim is to mitigate potential harm to end users. Bob Diachenko leans on his extensive cybersecurity experience to quickly uncover breaches, analyze the data, and track down the responsible organization.
- Once the database has been secured, we write a report like this one to help notify affected users and make them aware of the risks. We hope our work can make users safer and limit abuse by malicious parties.
- Source: Comparitech 7 million Adobe Creative Cloud accounts exposed to the public - Comparitech

Conclusion

Adobe

For its part, Adobe admitted to the leaky server in a blog post Friday, October 25.
The cloud-based software company blamed the incident on a misconfiguration to one of its "prototype environments" that led to the server becoming exposed on the internet.
This leak is nowhere as severe as the infamous 2013 Adobe breach, where hackers obtained full records, including encrypted payment details, for nearly 38 million Adobe users.